REMARKS

Applicant respectfully requests reconsideration and allowance of the subject application in view of the foregoing amendments and the following remarks.

Claims 1-73 are pending in the application, with claims 1, 13, 24, 36, 42, 48, 57, and 65 being independent. Claims 1, 5, 13, 17, 24, 36, and 42 are amended herein. Claims 48-73 were previously withdrawn from consideration. Support for the claim amendments and additions can be found in the original disclosure, particularly, for example, on pages 18-20. No new matter is added.

CLAIM OBJECTIONS

Claims 5-7, 17-19, & 36-47 stand objected to because of informalities. Claims 5, 17, 36, and 42 are amended herein to address the informalities noted in the Office Action. Accordingly, Applicant requests withdrawal of the claim objections.

§ 102 REJECTIONS

Claims 1-7 & 36-41 stand rejected under 35 U.S.C. § 102(b) as being anticipated by *"Short Signatures from the Weil Pairing"* by Boneh et al. (Boneh), published December 9-13, 2001.

Applicant respectfully traverses the rejection.

Nevertheless, without conceding the propriety of the rejection and in the interest of expediting allowance of the application, claim 1 has been amended and is believed to be allowable.

Independent claim 1, as presently presented, recites:

> A method comprising:
> identifying data to be signed;
> establishing parameter data for use with signature generating logic that encrypts data based on a Jacobian of a curve within a family of curves, said Jacobian having a genus exceeding two, said parameter data causing said signature generating logic to select at least one Gap Diffie-Hellman (GDH) group of elements relating to said curve within a family of curves;
> determining private key data and corresponding public key data using said signature generating logic; and
> signing said identified data with said private key data to create a corresponding digital signature.

Boneh is directed to short digital signatures in environments where a human is asked to manually key in the signature (Boneh, page 514), and discloses a short signature scheme based on the Computational Diffie-Hellman assumption on certain elliptic and hyper-elliptic curves (Boneh, Abstract). Boneh states "[i]t is an open problem whether one can build a family of hyper-elliptic curves of genus 3 that would give short signatures with higher security." (Boneh, p525) Boneh fails to teach the use of hyper-elliptic curves of genus 3 or higher in this fashion. Boneh also fails to disclose selecting the curve from a family of curves. Boneh further fails to teach "generating logic that encrypts data based on a Jacobian of a curve within a family of curves, said Jacobian having a genus exceeding two," as presently recited in independent claim 1. Accordingly, claim 1 is allowable.

Dependent claims 2-7 depend from independent claim 1 and are allowable by virtue of this dependency, as well as for additional features that they recite.

Independent claim 36, as presently presented, recites:

> A method comprising:
> receiving message data and a corresponding digital signature and public key data;
> using parameter data to configure signature verifying logic that performs cryptography operations based on a Jacobian of a curve within a family of curves, said Jacobian having a genus greater than two, said parameter data causing said signature verifying logic to select at least one Gap Diffie-Hellman (GDH) group of elements relating to said curve within a family of curves; and
> with said signature verifying logic, determining if said digital signature is valid using said public key data and said message data.

Boneh is directed to short digital signatures in environments where a human is asked to manually key in the signature (Boneh, page 514), and discloses a short signature scheme based on the Computational Diffie-Hellman assumption on certain elliptic and hyper-elliptic curves (Boneh, Abstract). Boneh states "[i]t is an open problem whether one can build a family of hyper-elliptic curves of genus 3 that would give short signatures with higher security." (Boneh, p525) Boneh fails to teach the use of hyper-elliptic curves of genus 3 or higher in this fashion. Boneh also fails to disclose selecting the curve from a family of curves. Boneh further fails to teach "using parameter data to configure signature verifying logic that performs cryptography operations based on a Jacobian of a curve within a family of curves, said Jacobian having a genus greater than two," as presently recited in independent claim 36. Accordingly, claim 36 is allowable.

Dependent claims 37-41 depend from independent claim 36 and are allowable by virtue of this dependency, as well as for additional features that they recite.

§ 103 Rejections

Claims 13-19, 24-30, & 42-47 stand rejected under 35 U.S.C. § 103(a) as being unpatenable over **Boneh** "in view of what is well known in the art." (Office Action, page 6.)

Applicant respectfully traverses the rejection. Nevertheless, without conceding the propriety of the rejection and in the interest of expediting allowance of the application, claims 13, 24, and 42 have been amended and are believed to be allowable.

Independent claim 13, as presently presented recites:

> A computer-readable medium having computer implementable instructions for causing at least one processing unit to perform acts comprising:
> providing signature generating logic capable of digitally signing identified data;
> configuring said signature generating logic using parameter data, said signature generating logic being configured to digitally sign said identified data based on a Jacobian of a curve <u>within a family of curves</u>, said Jacobian having a genus greater than <u>two</u>, said parameter data causing said signature generating logic to select at least one Gap Diffie-Hellman (GDH) group of elements relating to said curve <u>within a family of curves</u>;
> determining private key data and corresponding public key data using said signature generating logic; and
> signing said identified data with said private key data using said signature generating logic to create a corresponding digital signature.

Boneh is directed to short digital signatures in environments where a human is asked to manually key in the signature (Boneh, page 514), and discloses a short signature scheme based on the Computational Diffie-Hellman assumption on certain elliptic and hyper-elliptic curves (Boneh, Abstract). Boneh states "[i]t is an open problem whether one can build a family of hyper-elliptic curves of genus 3 that would give short signatures with higher security." (Boneh, p525) Boneh fails to teach the use of hyper-elliptic curves of genus 3 or higher in this fashion. Boneh also fails to disclose selecting the curve from a family of curves. Boneh further fails to teach "configuring said signature generating logic using parameter data, said signature generating logic being configured to digitally sign said identified data based on a Jacobian of a curve <u>within a family of curves</u>, said Jacobian having a genus greater than <u>two</u>," as presently recited in independent claim 13. Accordingly, claim 13 is allowable.

Dependent claims 14-19 depend from independent claim 13 and are allowable by virtue of this dependency, as well as for additional features that they recite.

Independent claim 24, as presently presented recites:

> An apparatus comprising:
> memory configured to store identifying data that is to be signed;
> signature generating logic that encrypts data based on a Jacobian of a curve <u>within a family of curves</u>, said Jacobian having a genus greater than <u>two</u>, said signature generating logic being operatively coupled to said memory and configurable using parameter data, said parameter data causing said signature generating logic to select at least one Gap Diffie-Hellman (GDH) group of elements relating to said curve <u>within a family of curves</u>, and wherein said signature generating logic determines private key data and corresponding public key data, and then signs said identified data with said private key data to create a corresponding digital signature.

Boneh is directed to short digital signatures in environments where a human is asked to manually key in the signature (Boneh, page 514), and discloses a short signature scheme based on the Computational Diffie-Hellman assumption on certain elliptic and hyper-elliptic curves (Boneh, Abstract). Boneh states "[i]t is an open problem whether one can build a family of hyper-elliptic curves of genus 3 that would give short signatures with higher security." (Boneh, p525) Boneh fails to teach the use of hyper-elliptic curves of genus 3 or higher in this fashion. Boneh also fails to disclose selecting the curve from a family of curves. Boneh further fails to teach "signature generating logic that encrypts data based on a Jacobian of a curve <u>within a family of curves</u>, said Jacobian having a genus greater than <u>two</u>," as presently recited in independent claim 24. Accordingly, claim 24 is allowable.

Dependent claims 25-30 depend from independent claim 24 and are allowable by virtue of this dependency, as well as for additional features that they recite.

Independent claim 42, as presently presented recites:

> A computer-readable medium having computer implementable instructions for causing at least one processing unit to perform acts comprising:
> receiving message data and a corresponding digital signature and public key data;
> using parameter data <u>to</u> configure signature verifying logic that performs cryptography operations based on a Jacobian of a curve <u>within a family of curves</u>, said Jacobian having a genus greater than <u>two</u>, said parameter data causing said signature verifying logic to select at least one Gap Diffie-Hellman (GDH) group of elements relating to said curve <u>within a family of curves</u>; and
> with said signature verifying logic, determining if said digital signature is valid using said public key data and said message data.

Boneh is directed to short digital signatures in environments where a human is asked to manually key in the signature (Boneh, page 514), and discloses a short signature scheme based on the Computational Diffie-Hellman assumption on certain elliptic and hyper-elliptic curves (Boneh, Abstract). However, Boneh fails to disclose or suggest "using parameter data <u>to</u> configure signature verifying logic that performs cryptography operations based on a Jacobian of a curve within a family of curves, said Jacobian having a genus greater than two," as presently recited in claim 42.

Dependent claims 43-47 depend from independent claim 42 and are allowable by virtue of this dependency, as well as for additional features that they recite.

Claims 8-12 stand rejected under 35 U.S.C. § 103(a) as being unpatenable over **Boneh.**

Claims 8-12 depend from independent claim 1. Applicant respectfully traverses the rejection. Nevertheless, without conceding the propriety of the rejection and in the interest of expediting allowance of the application, claim 1 has been amended and is believed to be allowable.

For the reasons stated above, independent claim 1 is allowable. Therefore, claims 8-12 are allowable by virtue of this dependency, as well as for additional features that they recite.

Claims 20-23 & 31-35 stand rejected under 35 U.S.C. § 103(a) as being unpatenable over **Boneh**, as modified above with respect to claims 13 & 24.

Applicant respectfully traverses the rejection. Claims 20-23 depend from independent claim 13 and claims 31-35 depend from independent claim 24. For the reasons stated above, independent claims 13 and 24 are believed to be allowable. Therefore, claims 20-23 and 31-35, respectively, are allowable by virtue of this dependency, as well as for additional features that they recite.

CONCLUSION

For at least the foregoing reasons, claims 1-47 are in condition for allowance. Applicant respectfully requests reconsideration and withdrawal of the rejections and an early notice of allowance.

If any issue remains unresolved that would prevent allowance of this case, **Applicant requests that the Examiner contact the undersigned attorney to resolve the issue**.

Respectfully submitted,

Date: 11/16/2007

By: ____________________
Christopher W Lattin
Reg. No. 56,064